

Приложения в контейнеры.
Угрозы за борт!

Ноябрь '24

Kaspersky Container Security

kaspersky активируй
будущее



Входит в

**Kaspersky
Cloud Workload
Security**



Контейнеризация

Один из главных мировых трендов в области разработки ПО. Технология позволяет ускорить процесс создания и доставки приложений, однако архитектурные особенности контейнерных сред не позволяют обеспечить их защиту традиционными решениями.

Защита контейнерных сред и повышение безопасности гибридной инфраструктуры организации

Kaspersky Container Security (KCS) — это решение, которое обеспечивает безопасность контейнерных приложений на всех этапах жизненного цикла: от разработки до эксплуатации. Продукт позволяет защитить бизнес-процессы организации, соответствовать стандартам и нормам безопасности, а также помогает реализовать принцип безопасной разработки ПО (DevSecOps).

С помощью Kaspersky Container Security можно высвободить ресурсы ИБ-службы для решения других задач и сократить время вывода продуктов на рынок благодаря всеобъемлющей защите от актуальных киберугроз и автоматизации проверок на соответствие требованиям.

Kaspersky Container Security спроектирован с учетом особенностей контейнерных сред и обеспечивает защиту на разных уровнях: от образов контейнеров до ОС хоста.

Kaspersky Container Security является частью комплексного решения по защите облачных рабочих нагрузок Kaspersky Cloud Workload Security. Оно надежно защищает от кибератак и сокращает время обнаружения угроз и реагирования на них в облачных средах.

85%

компаний сталкивались с >1 инцидентом в Kubernetes за последние 12 месяцев*

39%

компаний сообщили об утечке данных из-за проблем с безопасностью контейнеров*

38%

компаний сталкивались с потерей доходов за последние 12 месяцев из-за проблем с безопасностью контейнеров*

Ключевые возможности



Встраивание в процесс разработки

- Интеграция с реестрами образов и платформами CI/CD
- Интеграция с системами безопасности и уведомлений



Защита оркестратора

- Обеспечение безопасности контейнеров в рантайме
- Интеграция с платформами оркестрации
- Отслеживание потребляемых ресурсов в кластере



Проверка на соблюдение требований регуляторов

- Проверка в соответствии с лучшими практиками безопасности
- Анализ уязвимостей по БДУ ФСТЭК и NIST

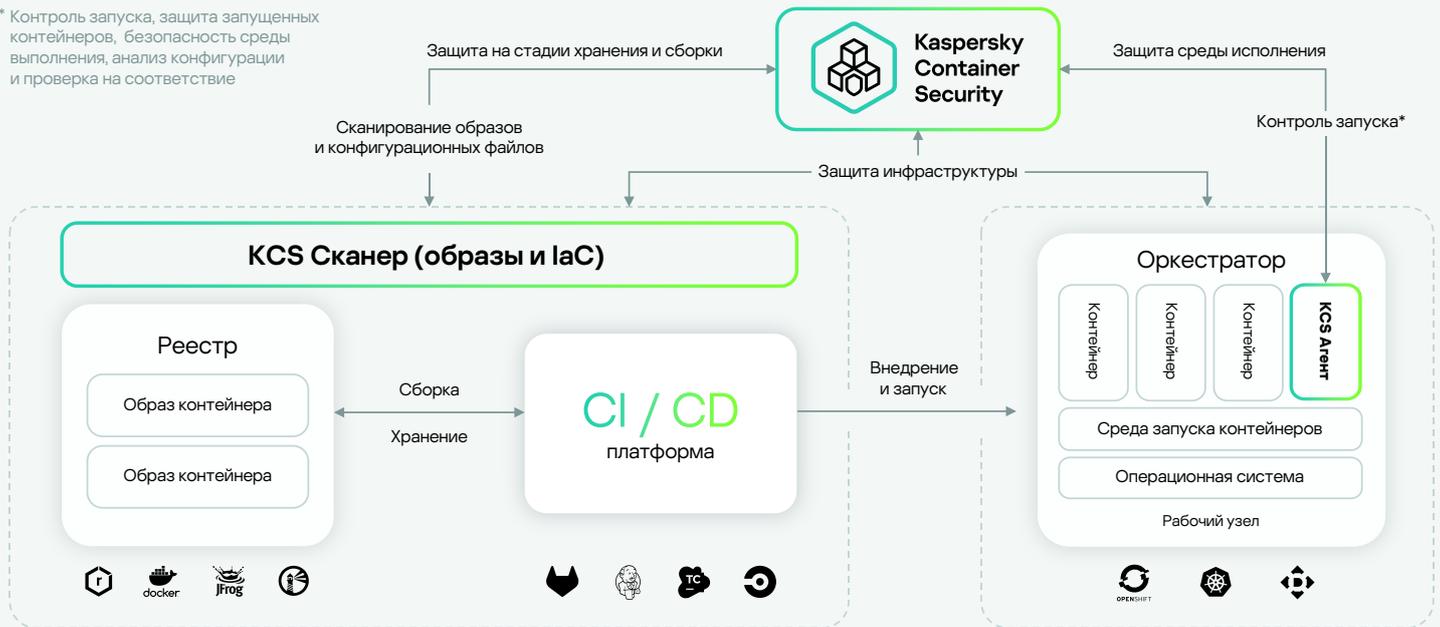


Визуализация и инвентаризация ресурсов в кластере

- Информативные дашборды и виджеты
- Наглядная инвентаризация ресурсов

Архитектура Kaspersky Container Security

* Контроль запуска, защита запущенных контейнеров, безопасность среды выполнения, анализ конфигурации и проверка на соответствие



Kaspersky Container Security (KCS) обеспечивает защиту на каждом этапе создания и эксплуатации приложения. KCS состоит из трех компонентов: KCS Агента, KCS Сканера и KCS Управляющего сервера.

KCS Сканер образов и инфраструктуры

Проверяет репозиторий на актуальность и безопасность образов. Кроме того, сканер позволяет проверять образ в рамках CI-процесса, снижая риски на этапе сборки. Устанавливается в кластер с серверными компонентами оркестратора.

KCS Агента

Обнаруживает уязвимости на уровне контейнеров, кластера, и оркестратора, обеспечивая безопасность среды выполнения. Агент устанавливается в кластер в виде обособленного контейнера на каждую ноду.

KCS Управляющий сервер

Отвечает за контроль состояния и взаимодействие компонентов продукта, а также за агрегацию информации об обнаруженных событиях. Устанавливается в кластер с серверными компонентами оркестратора.

Встраивание в процесс разработки



Преимущества для бизнеса



Безопасность мирового уровня

Возможности продукта соответствуют лучшим практикам защиты контейнерных сред

Качественная защита, подтвержденная международными наградами



Всеобъемлющая защита контейнерных сред

Защита на разных уровнях архитектуры контейнерных сред

Безопасность приложений на всех этапах жизненного цикла



Отечественное ПО

Решение от надежного российского вендора

В Реестре отечественного ПО (№16222)



Соответствие требованиям

Анализ уязвимостей по БДУ ФСТЭК

Поддержка ОС Astra Linux и РЕД ОС

Уровни и объекты лицензирования



Kaspersky Container Security

Standard

Предоставляет защиту образов контейнеров, интеграцию с реестрами образов, оркестраторами и CI/CD-платформами, а также с SIEM-системами



Kaspersky Container Security

Advanced

Обеспечивает защиту контейнеров в среде выполнения, предоставляет улучшенные возможности мониторинга и инструменты проверок на соответствие требованиям регуляторов

1 лицензия



1 нода с контейнерами*

* Учитываются ноды контейнерной инфраструктуры организации, на которых разворачивается агент защиты KCS Агент

Компонент Kaspersky Cloud Workload Security

Kaspersky Container Security вместе с Kaspersky Security для виртуальных и облачных сред входят в состав решения для всеобъемлющей защиты облачных нагрузок Kaspersky Cloud Workload Security. Это комплексное решение безопасности всей гибридной и облачной инфраструктуры клиентов: хостов, виртуальных машин, контейнеров, оркестраторов и других компонентов.



Совместимость

Kaspersky Security для виртуальных и облачных сред

Kaspersky Container Security

Public clouds



Orchestrators



Private clouds



Image registries



VDI platforms



CI / CD platforms



* В перспективе



Kaspersky Container Security

[Подробнее](#)

www.kaspersky.ru

© 2024 АО «Лаборатория Касперского». Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

[#kaspersky](#)
[#активируйбудущее](#)